(W)

DERWENT-ACC-NO: 1998-235992

DERWENT-WEEK: 200027

TITLE: Electronic voting method - involves signing contents of vote in election management apparatus after contents of vote with signature are confirmed in authentication computer

PATENT-ASSIGNEE: NIPPON TELEGRAPH & TELEPHONE CORP[NITE]

PRIORITY-DATA: 1988JP-0000642 (January 7, 1988) , 1997JP-0103784 (January 7, 1988)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
JP 10074046 A	March 17, 1998	N/A	010	G09C 001/00

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
JP 10074046A	Div ex	1988JP-0000642	January 7, 1988
JP 10074046A	N/A	1997JP-0103784	January 7, 1988

INT-CL (IPC): G06F019/00, G09C001/00

RELATED-ACC-NO: 2000-308927

ABSTRACTED-PUB-NO: JP 10074046A

BASIC-ABSTRACT:

The method entails obtaining unsigned votes through encryption. A random number generator, disturbance device and a random-number component removal device are provided in a vote content transmission device at a voter side. A signature function computer and an authentication computer serve as an election management apparatus at an election management side.

The vote content transmission device outputs a vote sentence and the contents of a vote to the disturbance device, and then transmits them to the election management apparatus. The signature function computer inputs the vote sentence and the corresponding signature is produced and then returned to the vote content transmission device. The random-number component removal device inputs the vote sentence with the signature to remove the random-number component and obtain a corresponding value that is transmitted to the election management apparatus. The authentication computer inputs the contents of the vote with the signature for confirmation, and the contents of the vote are signed by the election management apparatus.

ADVANTAGE - Detects if contents of vote are altered.

CHOSEN-DRAWING: Dwg.5/7

TITLE-TERMS: ELECTRONIC VOTE METHOD SIGN CONTENT VOTE MANAGEMENT APPARATUS AFTER CONTENT VOTE SIGNATURE AUTHENTICITY COMPUTER

DERWENT-CLASS: P85 T01

EPI-CODES: T01-D01; T01-J05A;

SECONDARY-ACC-NO:
Non-CPI Secondary Accession Numbers: N1998-187105

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－74046

(43)公開日　平成10年(1998)３月17日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ　1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６６０Ｚ	
	６４０	7259－5Ｊ		６４０Ｚ	
Ｇ０６Ｆ　19/00			Ｇ０６Ｆ　15/28	Ｂ	

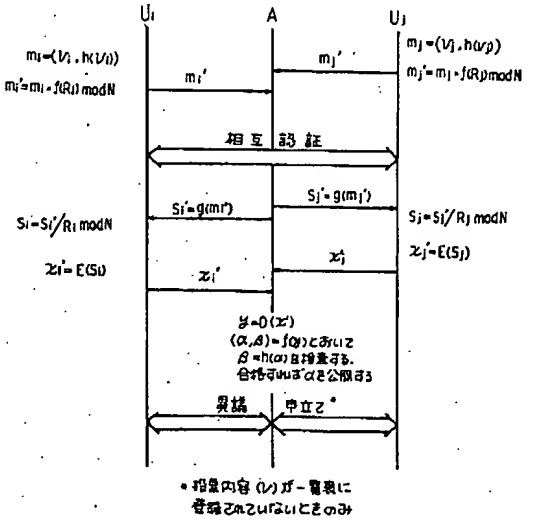
審査請求　有　　請求項の数７　書面　（全 10 頁）

(21)出願番号　特願平9－103784
(62)分割の表示　特願昭63－642の分割
(22)出願日　昭和63年(1988)１月７日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(72)発明者　太田　和夫
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　澤井　敬史

(54)【発明の名称】　電子投票方法

(57)【要約】
【課題】選挙管理者を１つだけ用いて安全かつ公平な電子投票方法を提供すること。
【解決手段】投票者Ｕは、投票文ｍｊを決め、これに乱数をかけて暗号化したｍｊ'を選挙管理者Ａに送る。次に、選挙管理者Ａは、投票権のある投票者Ｕからの投票である旨を確認するために、認証を行う。認証が行われたら、選挙管理者Ａは署名を行い、署名の付された署名付き投票文を暗号化して投票者Ｕに送る。投票者Ｕは、暗号化された署名付き投票文を平文（暗号を解いたもの）にする。この平文（Ｓｊ）に集計者だけが復号化できるもので暗号化したＸｊ'を選挙管理者Ａに送付する。



1

【特許請求の範囲】

【請求項１】暗号を用いて無記名投票を実現する電子投票方法において、

投票者側に乱数発生器と撹乱器と乱数成分除去器とから成る投票内容送信装置を備え、

選挙管理者側に署名関数計算器と認証関数計算器から成る選挙管理装置を備え、

前記投票内容送信装置は、前記乱数発生器を用いて生成した乱数成分と投票内容とを前記撹乱器に入力して撹乱された投票文を作成して前記選挙管理装置に送信し、

前記選挙管理装置は、撹乱された投票文を前記署名関数計算器に入力して署名付き投票文を作成して前記投票内容送信装置に送り返し、

前記投票内容送信装置は、署名付き投票文を前記乱数成分除去器に入力して乱数成分の影響を取り除いて投票内容に署名を施した値を求めた後にその値を前記選挙管理装置に送信し、

前記選挙管理装置は、署名付き投票内容を前記認証関数計算器に入力して投票内容が選挙管理者によって署名されているのを確認することにより無記名投票を実現することを特徴とする電子投票方法。

【請求項２】請求項１に記載の電子投票方法において、

前記各投票内容送信装置は、関数ｈを計算するｈ計算器（１３０）と連結器（１４０）とを更に備え、前記選挙管理装置は、関数ｈを計算するｈ計算器（２４０）と一致検査器（２５０）と投票内容一覧表とを更に備え、

各投票内容送信装置は、送信すべき投票内容をｖとするとき、ｖを前記ｈ計算器に入力して投票内容（ｖ）の関数ｈ（ｖ）を計算した後、前記連結器において前記関数ｈ（ｖ）と前記投票内容（ｖ）を連結することにより、投票文（ｍ）をｍ＝（ｖ，ｈ（ｖ））、即ちｖとｈ（ｖ）を並べたもの、として作成してこれを送信すべき投票内容として前記撹乱器に入力し、

選挙管理装置は、送信されてきた前記値（署名付きの、撹乱成分を除去された投票文）を認証関数計算器に入力し、その出力が、投票文（ｍ）の成分中の投票内容（ｖ）に対応する成分α、投票文（ｍ）の成分中の関数値ｈ（ｖ）に対応する成分β、から成る（α、β）で表されるとき、その中のαを前記ｈ計算器に入力して関数ｈ（α）を計算し、その値が前記βに一致するかを検査して、一致する場合にはαを投票内容として、前記投票内容一覧表に公開し、その公開された投票内容一覧表から投票内容の改ざんを検出可能にしたことを特徴とする電子投票方法。

【請求項３】暗号を用いて無記名投票を実現する電子投票方法において、

投票者側に乱数発生器と撹乱器と乱数成分除去器とから成る投票内容送信装置を備え、

選挙管理者側に署名関数計算器と認証関数計算器から成る選挙管理装置を備え、該投票内容送信装置は、前記乱数発生器を用いて生成した乱数成分と投票内容とを前記撹乱器に入力して撹乱された投票文を作成して該選挙管理装置に送信し前記選挙管理装置は、投票者の正当性を認証し、

前記選挙管理装置は、撹乱された投票文を前記署名関数計算器に入力して署名付き投票文を作成して前記投票内容送信装置に送り返し、

前記投票内容送信装置は、署名付き投票文を前記乱数成分除去器に入力して乱数成分の影響を取り除いて投票内容に署名を施した値を求めた後にその値を前記選挙管理装置に送信し、

前記選挙管理装置は、署名付き投票内容を前記認証関数計算器に入力して投票内容が選挙管理者によって署名されているのを確認することにより無記名投票を実現することを特徴とする電子投票方法。

【請求項４】請求項３に記載の電子投票方法において、

前記各投票内容送信装置は、関数ｈを計算するｈ計算器（１３０）と連結器（１４０）とを更に備え、前記選挙管理装置は、関数ｈを計算するｈ計算器（２４０）と一致検査器（２５０）と投票内容一覧表とを更に備え、

各投票内容送信装置は、送信すべき投票内容をｖとするとき、ｖを前記ｈ計算器に入力して投票内容（ｖ）の関数ｈ（ｖ）を計算した後、前記連結器において該関数ｈ（ｖ）と前記投票内容（ｖ）を連結することにより、投票文（ｍ）をｍ＝（ｖ，ｈ（ｖ））、即ちｖとｈ（ｖ）を並べたもの、として作成してこれを送信すべき投票内容として前記撹乱器に入力し、

選挙管理装置は、送信されてきた前記値（署名付きの、撹乱成分を除去された投票文）を認証関数計算器に入力し、その出力が、投票文（ｍ）の成分中の投票内容（ｖ）に対応する成分α、投票文（ｍ）の成分中の関数値ｈ（ｖ）に対応する成分β、から成る（α、β）で表されるとき、その中のαを前記ｈ計算器に入力して関数ｈ（α）を計算し、その値が前記βに一致するかを検査して、一致する場合にはαを投票内容として、前記投票内容一覧表に公開し、その公開された投票内容一覧表から投票内容の改ざんを検出可能にしたことを特徴とする電子投票方法。

【請求項５】暗号を用いて無記名投票を実現する電子投票方法において、

投票者側に乱数発生器と撹乱器と乱数成分除去器とから成る投票内容送信装置を備え、

選挙管理者側に署名関数計算器と認証関数計算器から成る選挙管理装置を備え、該投票内容送信装置は、前記乱数発生器を用いて生成した乱数成分と投票内容とを前記撹乱器に入力して撹乱された投票文を作成して該選挙管理装置に送信し、

前記選挙管理装置及び前記投票内容送信装置は、投票者の正当性を認証し、

前記選挙管理装置は、撹乱された投票文を前記署名関数

計算器に入力して署名付き投票文を作成して前記投票内容送信装置に送り返し、
前記投票内容送信装置は、署名付き投票文を前記乱数成分除去器に入力して乱数成分の影響を取り除いて投票内容に署名を施した値を求めた後にその値を前記選挙管理装置に送信し、
前記選挙管理装置は、署名付き投票内容を前記認証関数計算器に入力して投票内容が選挙管理者によって署名されているのを確認することにより無記名投票を実現することを特徴とする電子投票方法。

【請求項６】請求項５に記載の電子投票方法において、前記各投票内容送信装置は、関数ｈを計算するｈ計算器（１３０）と連結器（１４０）とを更に備え、前記選挙管理装置は、関数ｈを計算するｈ計算器（２４０）と一致検査器（２５０）と投票内容一覧表とを更に備え、
各投票内容送信装置は、送信すべき投票内容をｖとするとき、ｖを前記ｈ計算器に入力して投票内容（ｖ）の関数ｈ（ｖ）を計算した後、前記連結器において該関数ｈ（ｖ）と前記投票内容（ｖ）を連結することにより、投票文（ｍ）をｍ＝（ｖ，ｈ（ｖ））、即ちｖとｈ（ｖ）を並べたもの、として作成してこれを送信すべき投票内容として前記撹乱器に入力し、
選挙管理装置は、送信されてきた前記値（署名付きの、撹乱成分を除去された投票文）を認証関数計算器に入力し、その出力が、投票文（ｍ）の成分中の投票内容（ｖ）に対応する成分α、投票文（ｍ）の成分中の関数値ｈ（ｖ）に対応する成分β、から成る（α、β）で表されるとき、その中のαを前記ｈ計算器に入力して関数ｈ（α）を計算し、その値が前記βに一致するかを検査して、一致する場合にはαを投票内容として、前記投票内容一覧表に公開し、その公開された投票内容一覧表から投票内容の改ざんを検出可能にしたことを特徴とする電子投票方法。

【請求項７】請求項５又は６に記載の電子投票方法において、前記各投票内容送信装置は、通信回線を介して前記選挙管理装置に接続されている他の投票内容送信装置との間で、相互に身元を認証し合う相互認証手段を備え、それによって相互に身元を認証し合うことから投票内容送信装置の全数を知り、選挙管理装置による投票内容送信装置の数の人為的水増しがあれば、その検出を可能にしたことを特徴とする電子投票方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、電気通信システムでアンケート調査等を行う場合に、安全でかつ公平な無記名投票を実現する電子投票方法に関するものである。

【０００２】

【従来の技術】無記名投票は、投票者と投票内容の対応を秘密にでき、個人の思想信条に関するプライバシイを守るのに適しているので、電子会議やＣＡＴＶ等の双方向通信でのアンケート調査等に利用できる。

【０００３】電気通信において安全かつ公平な無記名投票を行うには、投票者の偽装や二重投票，投票文の盗聴に伴う投票内容の漏洩等の防止が必要である。これらの問題を解決する方法として、暗号を用いた電子投票方式が提案されている。

【０００４】例えば、［１］秋山稔他：“暗号を用いた無記名投票方式”，電子通信学会論文誌（Ａ），Ｊ６８－Ａ，１２，ｐｐ１２７８－１２８５（昭和５９－１２），［２］小山謙二：“ＲＳＡ公開鍵暗号を用いた無記名投票方式”電子通信学会論文誌（Ｄ），Ｊ６８－Ｄ，ｐｐ１９５６－１９６６（昭和６０－１１），［３］秋山稔他：“多重暗号化無記名投票方式”，電子通信学会論文誌（Ｂ），Ｊ６９－Ｂ，４，ｐｐ３１４－３２３（昭和６１－４）などがそれである。

【０００５】

【発明が解決しようとする課題】文献［１］で使用した暗号は安全でないので投票内容が漏洩し、無記名性（誰が何と投票したかを隠すこと）を保障できないので問題である。文献［２］では、安全なＲＳＡ暗号を用いて身元確認者と開票集計者を分離することによって無記名投票を実現する方式を提案している。

【０００６】しかし、身元確認者と開票集計者が結託した場合には、無記名性が保障できず、さらに選挙結果の不正操作が行える等の問題がある。文献［２］および［３］では、この問題に対する安全性を向上するために、身元確認者や開票集計者を複数にしたり、選挙管理委員会を身元確認者と開票集計者の間に配置する方式を提案している。

【０００７】しかし、これらの方法で十分な安全性を得るためには身元確認者，開票者，並びに委員を複数設ける必要が生じる。

【０００８】この発明の目的は、選挙管理者（身元確認者と開票者の機能を合わせ持つ）を１つだけ用いて安全かつ公平な電子投票方法を構築して提供することにある。

【０００９】

【課題を解決するための手段】上記目的達成のため、本発明では、投票者側に乱数発生器と撹乱器と乱数成分除去器とから成る投票内容送信装置を備え、選挙管理者側に署名関数計算器と認証関数計算器とから成る選挙管理装置を備えた。

【００１０】

【作用】この発明では、投票者が投票内容を乱数で撹乱して投票文を作成して、その結果を選挙管理者に送信する。選挙管理者は、投票文に署名して署名付き投票文を各投票者に送り返す。投票者は署名付き投票文から乱数の影響を取り除いた署名付き投票内容を求め、選挙管理者に送信する。選挙管理者は受信した署名付き投票内容が選挙管理者によって署名されていることを確認後に、

5

投票内容を公開する。それぞれの投票者は、公開された投票内容の一覧表に、自分の投票内容が登録されていることを確認し、登録されていない場合には、選挙管理者に対して異議を申し立てる。

【0011】ここで、投票文は投票内容に乱数が付加されているので、選挙管理者および第三者は投票文から投票内容を求めることが出来ず、投票の無記名性が保障できる。また、特に投票者の認証に相互認証を用いると、それぞれの投票者は投票者全体を知らされており投票数を知っているので、選挙管理者が不正に投票文を混ぜることは出来ない。さらに、選挙管理者が投票内容を改ざんしても、公開された投票内容の一覧表を用いて、投票内容の改ざんを検出可能である。

6

*【0012】以上より、この発明では従来より指摘されていた身元確認者と開票者が結託した不正行為である無記名性の喪失と選挙結果の不正操作の問題を解決できる。

【0013】

【発明の実施の形態】以下、説明の便宜上、投票者、選挙管理者という用語を使うが、これは実際は投票内容送信装置、選挙管理装置の意味であり、また投票というのは投票内容の送信を意味するものであることをお断りしておく。

【0014】第1図は、この発明の実施例の理解に役立つ原理構成図である。同図はL人の

*投票者$U_i(1 \le i \le L)$が通信回線を介して選挙管理者Aと接続している場合を表す。以下では、特に投票者Uが投票内容vを選挙管理者Aに対して投票する場合について説明する。

【0015】選挙管理者Aは、

$f(g(x))=g(f(x))=x$, $g(x \times y)=g(x) \times g(y)$,

かつfからgを求めるのが難しい2つの関数の組（f，g）を選んで、関数fを公開し、関数gを秘密にする。

【0016】この性質をみたす関数として、例えばRSA暗号の暗号化関数と復号化関数がある。RSA暗号（Rivest, R. L. etal.〝A Method for Obtaining Digital Signatures andPublic-Key Cryptosystems〟, Communications of the ACM, Vol. 21, No 2, pp. 120-126, (1978)）を用いた（f，g）の構成例は以下の通りである。

【0017】選挙管理者Aは、暗号化鍵（e，N）と復※

※号化鍵（d，N）を

$N=P \times Q$

$e \times d \equiv 1 \pmod{L}$

ただし　$L=LCM\{(P-1),(Q-1)\}$

をみたすように生成し、暗号化鍵を公開し、復号化鍵を秘密に管理する。

【0018】ここで、LCM｛a，b｝は整数aとbの最小公倍数を表して、PとQは相異なる2つの大きな素数とする。また、$a \equiv b \pmod{L}$は、a－bがLの倍数であることを表す。

【0019】RSA暗号は、Nが大きいときNの素因数分解が困難なことに安全性の根拠を持つ暗号であり、公開された暗号化鍵（N，e）から秘密の復号化鍵のd成分を求めることは困難である。

【0020】暗号化関数fと復号化関数gを

$f(M)=M^e \pmod{N}$

$g(C)=C^d \pmod{N}$

で定義すると、$0 \le x < N$をみたす整数xに対して

$g(f(x))=f(g(x))=x$

が成り立つことが示せる。ここで、$a \pmod{N}$は、aをNで割ったときの余りを表す。さらに、$0 \le x, y < N$をみたす整数x，yに対して

$g(x \times y)=g(x) \times g(y)$

が成り立つことが示せる。

【0021】以下では、関数gを署名関数，関数fを認証関数として用い、h（x）からxを求めるのが困難な一方向性関数hを公開する。特に、fとgとしてRSA暗号を用いる場合のf計算器とg計算器の効率のよい計算方法は、例えば池野，小山〝現代暗号理論〟電子通信学会，pp. 16－17，（1986）に示されている。また、h計算器の構成例を第2図に示す。第2図については特に説明を要しないであろう。

【0022】投票者Uのブロック構成図を第3図に示す。投票者Uは、次の手順を実行する。

STEP1：乱数発生器（110）を用いて乱数Rを生★

★成し、撹乱器（120）に引き継ぐ。

STEP2：120は関数fを計算するf計算器（121）を用いてf（R）を求め、乗算器（122）に引き継ぐ。

STEP3：連結器（140）は、関数hを計算するh計算器（130）を用いて求めたh（v）と自分の乱数成分を付加した投票内容v（つまり、vは立候補者の名前や賛成、反対等に自分の乱数成分を加えたものとなる）を連結して投票文m＝（v，h（v））を作成して乗算器（122）に引き継ぐ。

STEP4：122はmとf（R）を整数とみなし、公開されたNを用いて撹乱された投票文m'を

$m' = m \times f(R) \pmod{N}$

で暗号化して、IDと共に選挙管理者Aに送信する。選挙管理者Aが投票者Uの身元確認を行う場合には、署名生成器を用いて投票文m'に投票者Uの署名をつけて、Aに送信する。選挙管理者Aのブロック構成を第4図に

7

示す。選挙管理者Aは次の手順を行う。

【0023】STEP5：すべての投票者の間で相互認証を行う。（具体例は後述）選挙管理者Aが投票者Uの身元を確認する場合には、署名検査器を用いて、投票文m'に投票者Uの署名がついていることを検査する。

STEP6：署名関数gを計算する署名関数計算器としてのg計算器（210）を用いて投票文m'に対応する署名付き投票文s'を

s'＝g（m'）

で計算して、m'の送信元に送り返す。この操作をL個のすべての投票文に対して行う。投票者間の相互認証

8

＊（STEP5）の実施例としては、例えばE．F．Brickell他："N－Party Audio Secrecy，Identification and Signature" Globecome'87 Conference Record Vol．1of3，pp103－107がある。以下では、Brickell らの方法について説明する。

【0024】（STEP5の実施例）信頼できるセンタが、個人識別情報としてIDu j を用いる投票者に対して、次の手

順でk個の秘密情報$S_{u_j}(1 \le j \le k)$を生成する。

step5－1：一方向性関数hを用いて

$$V_{u_j} = h(ID_u, j)(1 \le j \le k)$$

を計算する。

step5－2：N'の素因数P'とQ'を用いてVu j に対して

$$S_{u_j} = \sqrt{(1/V_{u_j})} (\mathrm{mod}\, N')$$

を計算する。すなわち、Su j 2＝1／Vu j （mod N'）が成り立つようにSu j を選ぶ。

step5－3：投票者Uにk個のSu j を秘密に発行しN'を公開する。（modN'）における平方根の計算は、N'の素因数（P'とQ'）が分かっているときのみ実行できる。

【0025】その方法は、例えばRabin，M.　※O.："Digitalized Signatures and Public－Key Function asIntractable as Factorization"，Tech．Rep．MIT／LCS／TR－212 MIT Lab．comput．Sci．1979に示されている。平方根の計算装置の具体的な構成例は、公開鍵暗号システム（特願昭61－169350）に示されている。

【0026】それぞれの投票者は他のすべての投票者に対して自分が本物であることを証明するために、次の手順を実行する。

step5－4：投票者Uは乱数ru を生成して、

xu＝ru 2（modN'）

を計算してAに送る。

step5-5：Aは$X=\prod_{u=1}^{L} x_u (\mathrm{mod}\, N')$を計算してSTEP4で収集したIDから成る投票者リストΓと共にすべての投票者に送信する。

なお　$\prod_{u=1}^{L} x_u = x_1 \cdot x_2 \cdot x_3 \cdots\cdots x_L$である。

step5－6：投票者は受信したXとΓから

e＝h（X，Γ）

でビット列eを求め先頭のkビットを（e1，…，ek）とおく。

step5－7：投票者Uは署名文yu を

$$y_u = r_u \times \prod_{j=1}^{k} s_{u_j}^{e_j} (\mathrm{mod}\, N')$$

★で計算してAに送る。

step5-8：Aは$Y=\prod_{u=1}^{L} y_u (\mathrm{mod}\, N')$を計算してすべての投票者に送信する。

step5－9：投票者は

$$X = Y^2 \times \prod_{j=1}^{k} V_j^{e_j} (\mathrm{mod}\, N')$$

が成り立つかを検査する

（ただし、$V_j = \prod_{u=1}^{L} v_{u_j}$とする）。

yu の作り方よりyu 2 Π vu j ej ≡ru 2 Π（su j 2 ej × vu j ej）

≡ru 2

≡xu （modN'）であり、

☆

$$X \equiv \prod_{u=1}^{L} x_u \equiv \prod_{u=1}^{L} \left(y_u^2 \prod v_{u_j}^{e_j} \right)$$

$$\equiv \left(\prod_{u=1}^{L} y_u^2 \right) \left(\prod_{u=1}^{L} \prod_{j=1}^{k} v_{u_j}^{e_j} \right)$$

$$\equiv Y^2 \prod_{j=1}^{k} V_j^{e_j} (\mathrm{mod}\, N')$$

であるから、上の検査式に合格すると、L人の投票物は本物と確認できる。（STEP5の実現例　以上）

☆　投票者Uは、暗号化された署名付き投票文s'を受信すると次の手順を行う。

【0027】STEP7：STEP1で生成した乱数Rと公開されたNと選挙管理者から受信したs'を乱数成分除去器（150）に入力して

s＝s'／R（modN）

で通信文mに対する署名付き投票内容sを計算する。

STEP8：sを暗号器E（（160）に入力してx'を

x'＝E（s）

で求めて選挙管理者に送信する。選挙管理者は暗号化された署名付き投票内容x'を受信すると次の手順を行う。

STEP9：x'から復号器D（220）を用いて

y＝D（x'）

でyを求める。

STEP10：認証関数計算器としてのf計算器（230）を用いてf（y）を求め、v成分に対応する成分をα、h（v）に対応する成分をβとおく。

（α，β）＝f（y）

STEP11：h計算器（240）にαを代入してh（α）を求める。

STEP12：一致検査器（250）を用いてβ＝h（α）が成立するかを検査する。一致する場合、α成分を投票内容の一覧表に登録する。一致しない場合、誤りメッセージを出力する。

【0028】以上をまとめて得られる投票者と選挙管理者の間の交信例を第5図に示したので参照されたい。

【0029】投票者と選挙管理者の間の暗号通信に用いる（E，D）の実施例として、例えば、T. El Gamal:"A Public Key Cryptosystem and a Signature Scheme Based onDiscrcteLogarithms", IEEE Tran. IT 31, pp. 469－472（1985）やS. Goldwasser and S. Micali:"Probabilistic encryption", Journal of Computer and System Sciences, Vol. 28, 1984, pp. 270－299がある。以下では、ElGamalの方法を用いる場合について説明する。

【0030】選挙管理者は、Nの素因数であるPとQに対するガロア体GF（P）とGF（Q）の原始根gと

α＝g^β（modN）

で計算したαとN（＝P×Q）を公開して、βを秘密にする。投票者は乱数rを発生し、αと乱数rと公開情報Nを用いて

WK＝α^r（modN）

で秘密鍵WKを計算して、WK署名付き投票内容sの暗号化に使用する。同時に、投票者はrとNと原始根gを用いて

y＝g^r（modN）

で鍵配送成分yを計算して、暗号化した結果と共に選挙管理者に送信する。すなわち、

x'＝E（s）＝（y，sをWKで暗号化した値）

となる。

【0031】一方、選挙管理者は秘密のβと受信したyと公開情報Nから、

y^β（modN）

で秘密鍵WKを計算して、WK復号化する。投票者と選挙管理者で生成した秘密鍵WKが同じ値となることは、

α^r＝（g^β）^r

＝（g^r）^β

＝y^β

が成り立つことより明らかである。

【0032】最後に、投票者は公開された投票内容の一覧表を閲覧して、自分の投票内容が登録されていることを確認する。登録されていない場合には、選挙管理者に対して異議を申し立てる。ここで、正規のx'が一致検査に合格して、αがvとなる理由は、

s'＝g（m'）＝g（m×f（R））≡g（m）×g（f（R））（modN）≡g（m）×R（modN）

なので

y＝D（x'）＝D（E（s））＝s≡s'／R（modN）＝g（m）

となり

（α，β）＝f（y）＝f（g（m））＝m＝（v，h（v））

が成り立つことから明らかである。このようにαがvとなる場合は、αを公開することは、自分の乱数成分を付加した投票内容vを公開することに他ならないから、自分だけが知っている乱数成分を見て、自分の登録内容を確認できるのである。

【0033】

【発明の効果】この発明では、投票内容（v）と乱数（R）を撹乱して投票文（m'）を生成するので、選挙管理者および第三者は投票文から投票内容を求めることは出来ない。それぞれの投票者は投票者全体の相互認証をして投票者全体を知らされており投票総数を知っているので、選挙管理者が不正に投票文を混ぜることは出来ない。また、選挙管理者が投票内容を改ざんしても、公開された投票内容の一覧表を閲覧することで、投票内容の改ざんを検出できる。

【0034】以上より、この発明では投票者と選挙管理者間のプロトコルを工夫することで、1つの選挙管理者を設けるだけで、従来指摘されていた身元確認者と開票者が結託した場合の不正行為（無記名性の喪失と選挙結果の不正操作）を解決できる。

【0035】

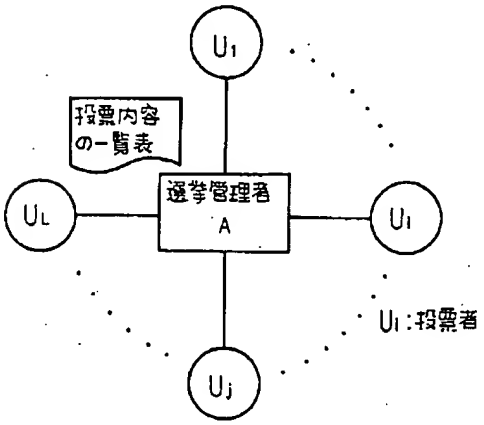
【図面の簡単な説明】

第1図はこの発明の実施例の理解に役立つ原理構成図、第2図はh計算器の実現例を示すブロック図、第3図は

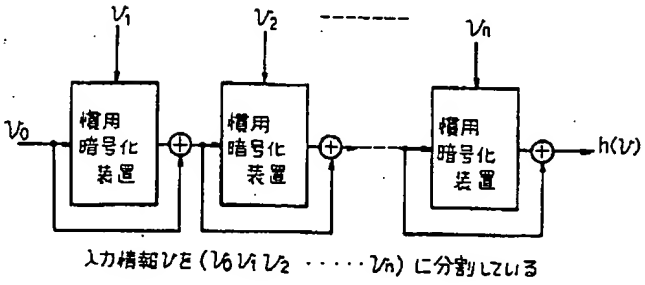
投票者を示すブロック図、第4図は選挙管理者を示すブロック図、第5図は投票者と選挙管理者間の交信例を示すチャート、第6図はシステム生成時の相互認証を示す

ブロック図、第7図は相互認証時のブロック説明図、である。

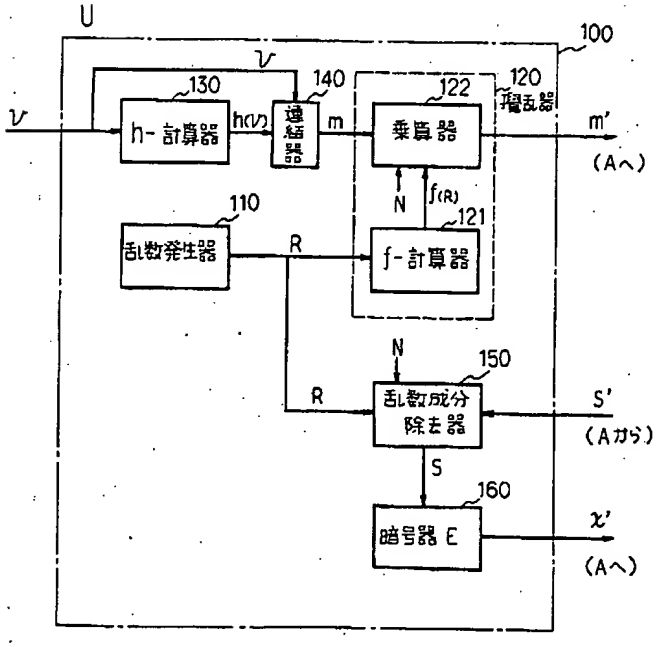
【第1図】



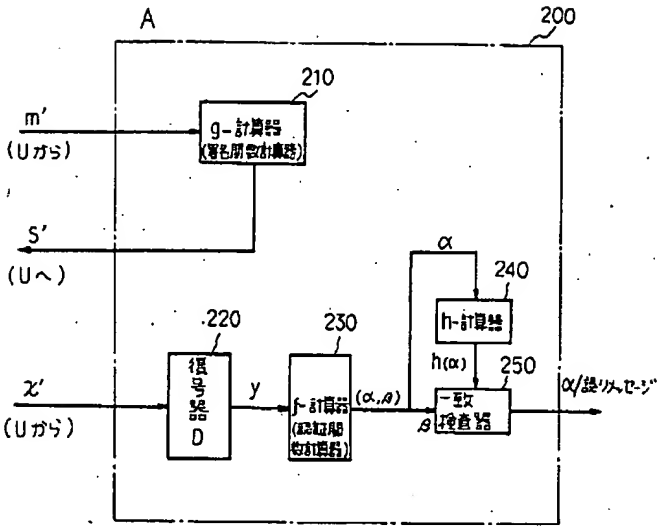
【第2図】



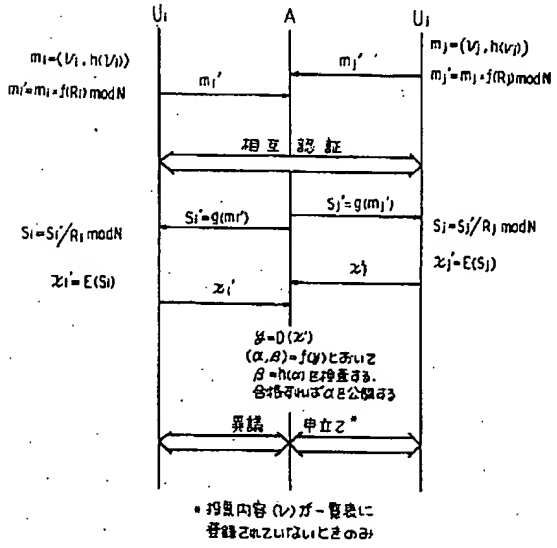
【第3図】



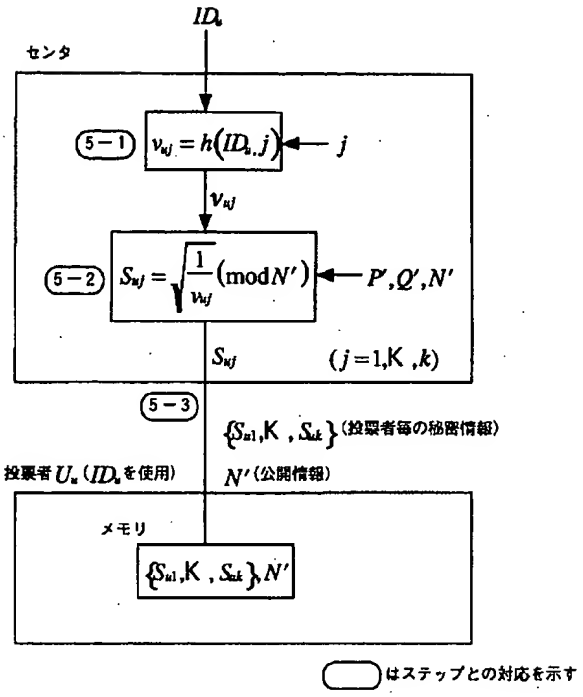
【第4図】


A
200
210
m'
(Uから)
g-計算器
(署名開設計算器)
S'
(Uへ)
α
240
h-計算器
220
230
h(α)
250
χ'
(Uから)
復号器 D
y
f-計算器
(認証開始計算器)
(α,β)
一致検査器
β
α/誤りメッセージ

【第5図】

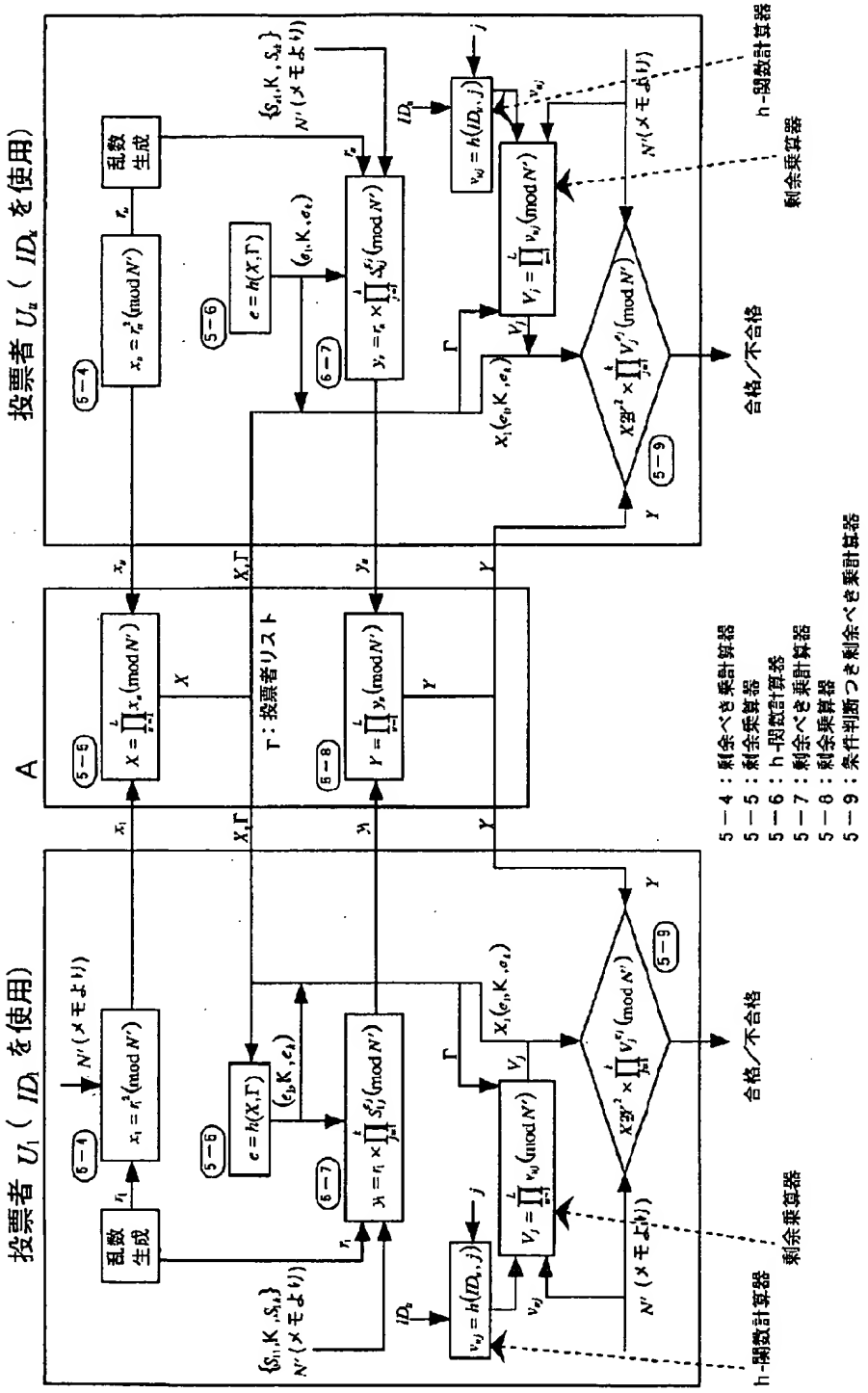

Ui
A
Uj
mi=(Vi, h(Vi))
mi'=mi・f(Ri) mod N
mi'
mj'
mj=(Vj, h(Vj))
mj'=mj・f(Rj) mod N
相互認証
Si'=g(mi')
Sj'=g(mj')
Si=Si'/Ri mod N
Sj=Sj'/Rj mod N
χi'=E(Si)
χj'
χi'
β=D(χ')
(α,β)=f(α)とおいて
β=h(α)を検査する.
合格すればαを公開する
異議
申立て*
*投票内容(V)がガー登表に
登録されていないときのみ

【第6図】



装置名称
5－1：h-関数計算器
5－2：剰余平方根計算器

【第7図】


投票者 U_1（ID_1 を使用）
投票者 U_n（ID_n を使用）
A
Γ：投票者リスト
乱数生成
h-関数計算器
剰余乗算器
合格／不合格
5－4：剰余べき乗計算器
5－5：剰余乗算器
5－6：h-関数計算器
5－7：剰余べき乗計算器
5－8：剰余乗算器
5－9：条件判断つき剰余べき乗計算器

第7図